**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 17/60, 1/00

A1

(11) International Publication Number: WO 00/57318

(43) International Publication Date: 28 September 2000 (28.09.00)

(21) International Application Number: PCT/CA00/00291

(22) International Filing Date: 17 March 2000 (17.03.00)

(30) Priority Data:
2,266,141 18 March 1999 (18.03.99) CA

(71) Applicant *(for all designated States except US)*: RDM CORPORATION [CA/CA]; 608 Weber Street North, Unit #4, Waterloo, Ontario M2V 1K4 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: FORDE, Peter, A. [CA/CA]; 11 Sugarbush Place, Guelph, Ontario N1H 7Z1 (CA). WALLACE, William, E. [CA/CA]; 97 William Street West, Waterloo, Ontario N2L 1J6 (CA). AKISTER, Jim, F. [CA/CA]; 149 Belmont Avenue, Waterloo, Ontario N2L 2B2 (CA).

(74) Agents: CURRIER, T., Andrew et al.; Gowling Lafleur Henderson LLP, Suite 4900, Commerce Court West, Toronto, Ontario M5L 1J3 (CA).

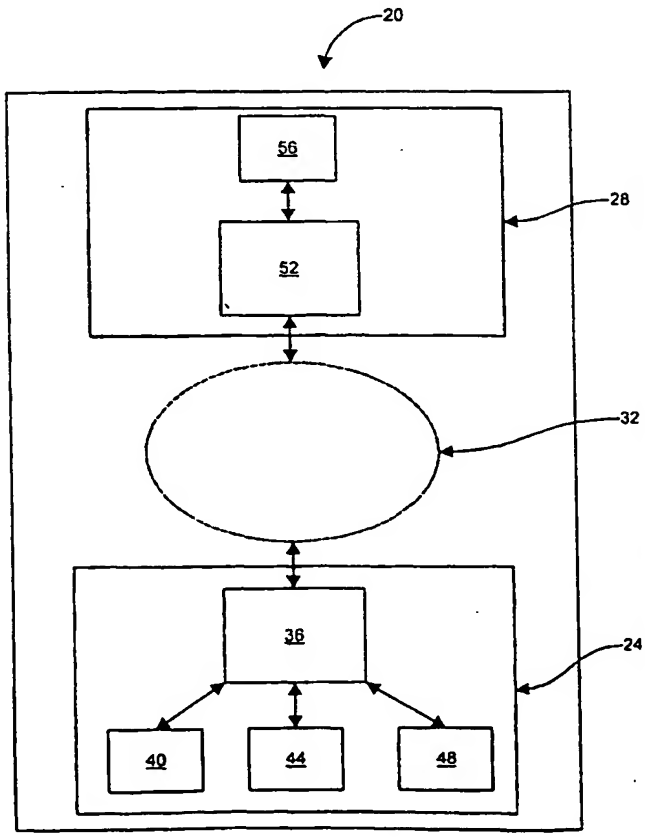
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*
*Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

(54) Title: METHOD AND SYSTEM FOR PROCESSING ELECTRONIC DOCUMENTS

(57) Abstract

The present invention provides a computer-based method and system for applying a set of business signing rules for the processing of electronic documents. The method includes the steps of verifying the identity of an authorized user using a predefined verification protocol, determining a set of privileges associated with the authorized user, filling-in an electronic document in accordance with the privileges and based on inputs provided by the authorized user, attaching a digital signature to the electronic document, and transmitting the electronic document to an authorized recipient of the electronic documents in accordance with the privileges.



*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AL | Albania | ES | Spain | LS | Lesotho | SI | Slovenia |
| AM | Armenia | FI | Finland | LT | Lithuania | SK | Slovakia |
| AT | Austria | FR | France | LU | Luxembourg | SN | Senegal |
| AU | Australia | GA | Gabon | LV | Latvia | SZ | Swaziland |
| AZ | Azerbaijan | GB | United Kingdom | MC | Monaco | TD | Chad |
| BA | Bosnia and Herzegovina | GE | Georgia | MD | Republic of Moldova | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagascar | TJ | Tajikistan |
| BE | Belgium | GN | Guinea | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan |
| BF | Burkina Faso | GR | Greece | | | TR | Turkey |
| BG | Bulgaria | HU | Hungary | ML | Mali | TT | Trinidad and Tobago |
| BJ | Benin | IE | Ireland | MN | Mongolia | UA | Ukraine |
| BR | Brazil | IL | Israel | MR | Mauritania | UG | Uganda |
| BY | Belarus | IS | Iceland | MW | Malawi | US | United States of America |
| CA | Canada | IT | Italy | MX | Mexico | UZ | Uzbekistan |
| CF | Central African Republic | JP | Japan | NE | Niger | VN | Viet Nam |
| CG | Congo | KE | Kenya | NL | Netherlands | YU | Yugoslavia |
| CH | Switzerland | KG | Kyrgyzstan | NO | Norway | ZW | Zimbabwe |
| CI | Côte d'Ivoire | KP | Democratic People's Republic of Korea | NZ | New Zealand | | |
| CM | Cameroon | | | PL | Poland | | |
| CN | China | KR | Republic of Korea | PT | Portugal | | |
| CU | Cuba | KZ | Kazakstan | RO | Romania | | |
| CZ | Czech Republic | LC | Saint Lucia | RU | Russian Federation | | |
| DE | Germany | LI | Liechtenstein | SD | Sudan | | |
| DK | Denmark | LK | Sri Lanka | SE | Sweden | | |
| EE | Estonia | LR | Liberia | SG | Singapore | | |

# METHOD AND SYSTEM FOR PROCESSING ELECTRONIC DOCUMENTS

## FIELD OF THE INVENTION

The present invention relates to the processing of electronic documents and the security issues pertaining thereto.

## BACKGROUND OF THE INVENTION

Paper-based business documents for carrying out commercial transactions are known. Paper-based documents include purchase orders, company invoices, or cheques. Paper-based documents usually incorporate an approval and/or verification procedure to reduce the likelihood of misallocation, theft, or misappropriation during the commercial transaction. Such approval and verification procedures typically involve the application of written signatures by various individuals processing the document. Generally a paper-based document requires the signature of more than one person. For example, an employee may require signatures from a supervisor, a manager, a controller or accountant and a purchaser for purchasing a single item. In the case of higher value transactions, additional signatures may be required.

There are many problems with the use of the paper-based business document. In particular, acquiring the signatures of each of the trusted individuals may be time consuming, requiring several hours or days before an order is finally placed. The delay may be further compounded in cases where signatures may be required by individuals at alternate locations. In today's global economy, signatures may be required from individuals in different states or even different countries. Therefore a paper-based business document must be sent to the locations of the individuals whose signature is required. Also, signatures may be required by managers or executives who are out of the office, for instance, on business travel making their approval unavailable until their return. Obtaining signatures on a paper-based document can be difficult and can delay important purchases. This can result in a delay to important and time-critical projects or work.

Another problem of the paper-based document is that paper-based documents may require translation for one or more persons. As stated, signatures may be required from individuals in different states or even different countries. Therefore, individuals signing a single paper-based document may speak different languages and may not understand the language on the document.

A translator may be required to understand a paper-based document. For example, an individual whose signature is required on a purchase order or a person receiving a purchase order may require translation of the document.

Yet another problem with paper-based documents is that a person seeking approval signatures need to determine who is authorized to approve the document, which can lead to additional delays in processing the document.

Another problem with paper-based documents is that each document may include several carbon copies for each of the departments concerned. For example, a person or department purchasing goods may receive a copy of a purchase order to confirm the order has been placed and to receive an estimated delivery date or other pertinent information included on the document. A supervisor or manager may receive copies of the purchase order for departmental budgeting. A financial department may require a copy for accounting purposes. Still another copy may go to a shipping and receiving department for confirmation of receipt of ordered goods. To provide the necessary copies of the purchase order to each individual or department there may be a plurality of layers of paper and carbon copies for each purchase order. When writing on the order form, the information may not be transferred to all of the copies. It can be difficult getting accurate imprints on each copy and forms may therefor be difficult to read or useless to the receiver of the copy. Further, a signature on a paper-based document may not be transferred to all of the copies of the document or may be difficult to decipher.

Yet another problem with paper-based documents is that individuals may attempt to forge a document. For example, a manager may sign several paper-based documents each day. In an attempt to expedite the process of signing several paper-based documents, the manager's signature may become less decipherable. A signature that is difficult to decipher may be easily forged. The forgery may be very difficult to detect and thus the approval or verification procedure of obtaining each signature can be circumvented. This can increase the likelihood of misallocation, theft or misappropriation.

Still another problem with paper-based documents is that they are generally not environmentally friendly as they can generate considerable waste. Further, documents with several copies can be very expensive for the company to purchase. Changes and updates to the paper-based document can be costly and can generate more waste. For example, a change in the format of the document may require redesign and reprinting. Also, each time a printer is required

to amend the documents there may be an additional cost to the company. Documents of the old format may be scrapped when the company implements the change, thus creating more waste.

It will now be apparent that similar problems can arise in a variety of paper-based document systems.

Computer systems and networks can offer certain ways to overcome some of the foregoing disadvantages, however, the verification procedure that is available in paper-based systems is not generally applicable to electronic systems.

## SUMMARY OF THE INVENTION

It is an object of the present invention to provide a novel documentation and signature application system that obviates or mitigates at least one of the disadvantages of the prior art.

The present invention is directed to a method for controlling the application of digital signatures to electronic documents based on electronically represented business signing rules which obviates or mitigates at least one problem not addressed by the prior art.

The rules are expressed electronically and referenced by a computer, rather than an individual, to route documents and control the application of the digital signatures. The computer can determine whether sufficient signatures have been obtained to conform to the businesses signing rules. The invention includes the design of a user interface which allows an administrator to create or modify signing and processing rules for multiple electronic documents and multiple signers at the same time.

The invention facilitates the electronic processing of transaction documents. It enables businesses to automate much of the labor-intensive processing of these documents.

In one embodiment of the invention, there is provided a computer-based method for configuring a set of digital business signing rules for the processing of electronic documents involving the application of a digital signature, said document created by at least one user, said method comprising the steps of:

a) establishing an identity and verification protocol for at least one system administrator

b) verifying the identity of one of said at least one administrator using said verification protocol

c) establishing an identity and verification protocol for said at least one user based on parameters provided by said verified administrator, and

d) establishing a set of privileges and authority levels associated with said electronic document for each of said at least one users based on parameters provided by said verified administrator

In a particular aspect of the first embodiment, there comprises the additional step of:

e) establishing at least one task for processing a batch of at least one type of said electronic documents

In a particular aspect of the first embodiment, the electronic document is an electronic financial instrument.

In another particular aspect of the first embodiment, the identity and verification protocol for said at least one user includes a smartcard.

In another particular aspect of the first embodiment, the identity and verification protocol for said at least one user includes a digital signature of the digital business rules pertaining to that user.

It is contemplated that other methods or means of verifying the integrity of the message and the identity the author which are essentially equivalent to digital signatures are within the scope of the invention.

In another particular aspect of the first embodiment, said privileges include the ability to create one or more different types of electronic documents.

In another particular aspect of the first embodiment, said privileges include the ability to edit one or more created electronic financial instruments.

In another particular aspect of the first embodiment, said privileges include the ability to schedule the further processing, including the transmission, of one or more created electronic financial instruments.

In another particular aspect of the first embodiment, said privileges include the ability to unilaterally approve one or more created electronic financial instruments.

In another particular aspect of the first embodiment, said privileges include the requirement that a created electronic financial instrument be co-signed by one or more users.

In another particular aspect of the first embodiment, said privileges include the ability to endorse a created electronic financial instrument.

In another particular aspect of the first embodiment, said privileges include the ability to authorize a created electronic financial instrument.

In another particular aspect of the first embodiment, said privileges include the ability to send a created electronic financial instrument.

In another particular aspect of the first embodiment, said privileges include the ability to hold a created electronic financial instrument.

In another particular aspect of the first embodiment, said privileges include the ability to print a created electronic financial instrument.

In a second embodiment of the invention, there is provided a computer-based method of applying a set of digital business signing rules for the processing of electronic documents, said method comprising the steps of:

a) verifying the identity of an authorized user using a predefined verification protocol;

b) determining a set of privileges associated with said authorized user;

c) creating an electronic document in accordance with said privileges and based on inputs provided by said authorized user;

d) attaching a digital signature to said electronic document; and

e) transmitting said electronic document to an authorized recipient of said electronic documents in accordance with said privileges;

In a particular aspect of the second embodiment, after the attachment of said digital signature performing the steps of:

requesting one or more additional authorized users to perform additional processing tasks for said electronic document;

attaching additional digital signatures complementary to said one or more additional authorized users upon fulfillment of said tasks of said electronic document;

In a third embodiment of the invention, there is provided a computer-based method of modifying a set of digital business signing rules for the processing of electronic documents, said method comprising the steps of:

a) verifying the identity of at least one authorized administrator using a predefined verification protocol;

b) determining a set of privileges associated with said verified at least one administrator;

c) modifying and/or establishing an identity and verification protocol for at least one user based on parameters provided by said verified at least one administrator, and

d) establishing a set of privileges and authority levels associated with said electronic documents for each of said at least one users based on parameters provided by said verified at least one administrator.

The present invention provides a novel method and system for processing electronic business documents. The present invention is believed to be particularly suitable for use in carrying out electronic commerce applications such as purchase orders, company invoices and company cheques. The system and method for processing electronic business documents can require less time to process than some traditional paper systems. The electronic document can be transferred quickly to those individuals in alternate locations and electronic signatures can be acquired very quickly. This includes individuals in other states or countries. Also, individuals who are out of the office can receive the electronic documents, (via, for example, a secure remote connection such as SSL) and associate his or her digital signature with the document and thus allowing for the approval of the document prior to their return to the office or work site. Thus delays to time-critical projects or work can be reduced. Electronic documents can easily be created in multiple languages or translated into a desired language. Copies or records of the electronic document can be saved or sent to each individual or department thus reducing the amount of paper and waste. Further, desired changes to the document can be made electronically and can reduce paper waste. Also, forgery of a document or signature and circumvention of the verification procedure can be more difficult. The present invention can also assist in the reduction of errors in the processing of electronic documents as the automatic routing of documents to appropriate individuals, and the control over the completion of the document in accordance with privileges can assist in avoiding routine errors during the preparation of the document. In addition, the automatic routing of the documents to the appropriate individuals (i.e. authorized users) can ensure a tighter control over the processing of the documents by keeping the document confidential and ensuring that only individuals who need to see the document are actually presented with the document.

## BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention will now be described, by way of example only, with reference to the attached Figures, wherein:

Figure 1 is a block diagram of a system for processing electronic business documents according to an embodiment of the invention;

Figure 2 is a representation of an electronic purchase order;

Figure 3 is a flow chart of a method for processing electronic business documents according to an embodiment of the invention;

Figure 4 is a flow chart of exemplary substeps for performing step 220 of Figure 3, in accordance to an embodiment of the invention; and

Figure 5 is the electronic purchase order of Figure 2 showing a representation of certain fields being completed thereon.

## DETAILED DESCRIPTION OF THE INVENTION

Referring to Figure 1, a system for processing electronic business documents, according to an embodiment of the invention, is indicated generally at 20. In the present embodiment, system 20 has a purchasing intranet 24 to generate an electronic business document and a vending intranet 28 for receiving the electronic business document. Purchasing and vending intranets 24, 28 are interconnected by a network 32.

Purchasing intranet 24 includes a purchasing server 36 and at least one intelligent device, preferably interconnected in client-server arrangement. In the present embodiment, there are three purchasing intelligent devices 40, 44, 48. Preferably, each purchasing intelligent device 40, 44, 48 is a personal computer. Purchasing intelligent devices 40, 44, 48 each include an input device such as a keyboard, an output device such as a video card and monitor, a processing unit, a random access memory, a persistent storage device, and a network interface card for connecting to server 36. Other intelligent devices, such as personal digital assistants, dumb-terminals, or thin-clients, can be used as will occur to those of skill in the art.

Purchasing server 36 includes an input device, an output device such as a video card and a monitor, a processing unit, a random access memory, a persistent storage device, and a network interface card for connecting to purchasing intelligent devices 40, 44, 48 and for connecting to network 32. Purchasing server 36 can send data to each purchasing intelligent device 40, 44, 48 and receive data from each purchasing intelligent device 40, 44, 48. A suitable server can be a Pentium-based Windows NT server, but other servers can be used as will occur to those of skill in the art.

Similar to purchasing intranet 24, vending intranet 28 includes a vending server 52 and at least one intelligent device. In the present embodiment, there is one vending intelligent device 56. Preferably, vending intelligent device 56 is a personal computer. Vending intelligent device 56 includes an input device such as a keyboard, an output device such as a video card and monitor, a processing unit, a random access memory, a persistent storage device, and a network interface card for connecting to vending server 52. Other intelligent devices, such as personal digital assistants, dumb-terminals, or thin-clients can be used, as will occur to those of skill in the art.

Vending server 52 includes an input device, an output device such as a video card and a monitor, a processing unit, a random access memory, and a persistent storage device, a network interface card for connecting to vending intelligent devices 56 and for connecting to network 32. Vending server 52 can send data to vending intelligent device 56 and receive data from vending intelligent device 52.

Purchasing server 36 and vending server 52 are interconnected by network 32. Purchasing server 36 and vending server 52 can exchange data via network 32. Network 32 can be any means of transferring data, such as a local area network, wide area network, the internet, or wireless.

System 20 is operable for processing at least one electronic document, such as an electronic purchase order, electronic invoices, or electronic cheques. In a present embodiment, system 20 is operable to process an electronic purchase order. Referring now to Figure 2, a representation of an electronic purchase order is indicated generally at 60. Electronic purchase order 60 includes a plurality of electronic data fields. In the present embodiment, electronic fields include a purchase order number field 64, a quantity field 68, an item field 72, a cost field 76, a date field 80, an approval field 81 and an issue filed 82. It will be understood that the fields 64, 68, 72, 76, 80, 81 and 82 of electronic purchase order 60 can be presented in any suitable user-interface on any of the intelligent devices in system 20.

Electronic purchase order 60 also includes data fields for identity verification of authorized users, of system 20 which in a present embodiment include a requester digital signature 84, an approver digital signature 88, and a purchaser digital signature 92. It will be understood that signatures 84, 88, 92 are generally not present on the user-interface, but are

stored as data that is associated with purchase order 60. The details of digital signatures 84, 88, 92 will be discussed in greater below.

Purchase order number field 64 is a reference number assigned by server 36 based on an operation that increments the reference number of the previous electronic purchase order. (Alternatively, the the purchase order number can be assigned through an application program interface using any desired means.) Quantity field 68 represents a desired quantity of items and can be entered by a requester from one of purchasing intelligent devices 40, 44, 48. Item field 72 represents a description of the desired items and can be entered by the requester. Cost field 76 represents a cost of the desired items and can be entered by the requester. Date field 80 indicates the date that the purchase order request was made and can be determined by purchasing server 36. Approval field 81 represents an approval or disapproval of electronic purchase order 60 and issue field 82 represents the issuance or non-issuance of electronic purchase order 60.

Server 36 is operable to store electronic purchase order 60 on its' persistent storage device in any suitable format, such as a database, and to make electronic purchase order 60 available for completion by an authorized user of one of purchasing intelligent devices 40, 44, 48. An authorized user can be any user from a user list stored on the persistent storage device of server 36.

In a present embodiment, server 36 is operable to determine whether a user is authorized using a smart-card system. Each person that is an authorized user carries a smart card unique to that authorized user. Each device 40, 44, 48 includes a reader operable to read each smart card. Server 36 is operable to determine whether a card has been inserted in a reader, and, upon entry of a password unique to the smart card, make the respective device available for use to the authorized user. Other systems of verifying the identity a user can be employed as will occur to those of skill in the art.

Server 36 is further operable to maintain a set of privileges associated with each authorized user. Such privileges can include, for example, the authority to complete certain data fields on electronic purchase order 60. In addition, privileges can include the authority to approve a maximum cost of the items as entered in cost field 76 and the issuance of electronic purchase order 60.

For the purposes of assisting in explaining embodiments of the present invention, Table I shows an exemplary list of authorized users and their associated privileges of purchasing intranet 24.

TABLE I

| Title | Name | Request Privilege | Approval | Issuance | Maximum Cost ($) |
|---|---|---|---|---|---|
| Requester | F. Smith | Yes | No | No | 5,000 |
| Requester | A. Johnson | Yes | No | No | 10,000 |
| Approver | D. Little | No | Yes | No | 10,000 |
| Approver | J. Adams | No | Yes | No | 10,000 |
| Purchaser | L. Carter | No | No | Yes | 10,000 |

As seen in Table I, privileges given to users F. Smith and A. Johnson include request privilege to a maximum cost of the items as entered in cost field 76 of $5000 and $10,000 respectively. Users D. Little and J. Adams have approval privileges for approving the purchase of items requested. User L. Carter has privilege for issuing electronic purchase order 60.

Purchasing server 36 is also operable to maintain a set of rules for the completion of electronic purchase order 60 by the authorized users. Such rules can include the sequence of completion of electronic purchase order 60. For example, it can be required that quantity field 68, item field 72 and cost field 76 are entered by the requester before an approver can receive and associate his or her digital signature 96 with electronic purchase order 60. Similarly, it can be required that the approver associates his or her digital signature 88 with purchase order 60 before a purchaser can associate his or her digital signature 92 with purchase order 60.

Purchasing server 36 is operable to transfer completed electronic purchase order 60 in accordance with privileges and rules programmed on server 36. In the present embodiment, electronic purchase order 60 is transferred to vending server 52. Purchasing server 36 and vending server 52 are interconnected by network 32 and electronic purchase order 60 is transferred using known data transfer communication protocols and techniques.

Vending server 52 is operable to receive electronic purchase order 60. Vending server 52 is further operable to make electronic purchase order 60 available to vending intelligent device 56 for a vending user to verify the authenticity and fill electronic purchase order 60.

A method for processing electronic business documents, according to another embodiment of the invention, will now be discussed with reference to system 20 and the flow chart shown in Figure 3. For the purposes of assisting in explaining the present embodiment, system 20, electronic purchase order 60 and the privileges in Table I will be used as an example.

Referring now to Figure 3, at step 200, the identity of the authorized user is verified. It will be assumed that F. Smith inserts his smart card into purchasing intelligent device 40 and enters his password into the user-input device of intelligent device 40. The entered password is then checked against the password stored on the smart-card, and, if verified, then F. Smith is granted access to purchasing intranet 24. Access is denied if F. Smith's identity is not verified. For the purpose of this example, the information from F. Smith's smart card matches an authorized user from the user list in Table I and purchasing intelligent device 40 is made available by server 36 for use by F. Smith.

At step 210, the authorized user's privileges are determined. As seen in Table I, possible privileges in the present example include request privilege, approval privilege, issuance privilege, and maximum cost privilege. In the present embodiment, server 36 determines that F. Smith is given request privilege to a maximum cost of $5000. Further, F. Smith is not given approval or issuance privilege.

At step 220, the electronic document is filled-out by the authorized user in accordance with the authorized user's privilege. F. Smith requests a blank electronic purchase order 60 and server 36 sends electronic purchase order 60 to purchasing intelligent device 40. A presently preferred set of sub-steps for performing step 220 is show in Figure 4. Referring now to Figure 4, purchasing intelligent device 40 receives a blank electronic purchase order 60 at step 221. F. Smith then enters data into quantity field 68, item field 72, and cost field 80. Referring now to Figure 5, for the purpose of explaining the present embodiment it will be assumed that F. Smith enters a number one in quantity field 68, "widget", in item field 72, and one-hundred dollars in cost field 76.

At step 222, server 36 then compares the data entered at step 221 with the privileges as determined at step 210 and determines whether F. Smith was authorized to enter the data that he entered. In the present example, server 36 determines that F. Smith has entered data that he was authorized to enter.

It is to be understood, for example, that if F. Smith had attempted to fill in an amount in cost field 76 greater than $5000.00, the method would move to step 223, the received document data would be rejected and the method would return to step 221. Similarly, if F. Smith attempted to enter any data that did not accord with his privileges, then the method would proceed to step 223, where the data that F. Smith attempted to enter would be rejected and the method would return to step 221. As F. Smith has entered data that he was authorized to enter, server 36 proceeds from step 222 to step 224 and assigns a date, typically using the internal date on server 36, in date field 80. A purchase order number is also assigned by server 36 to purchase order number field 68.

Referring again to Figure 3, at step 230, F. Smith's digital signature is associated with purchase order purchase order 60. Any known digital signature operations can be used. Details of these and other suitable digital signature concepts are discussed in "Electronic Payment Systems", Donal O'Mahony, Michael Peirce, Hitesh Tewari, © 1997, Artech House Incorporated ISBN 0890069255. Continuing with the present example, step 230 is accomplished as follows: Server 36 runs electronic purchase order 60 through a hashing operation which generates a unique fixed-length hash. The hash is then converted into a digital signature by encryption of the hash using an encryption key private to F. Smith. The digital signature is then affixed to electronic purchase order 60. F. Smith can only attach his digital signature to requester signature field 84 according the privileges as determined at step 210. Suitable hashing operations are also discussed in "Electronic Payment Systems".

At step 240, server 36 transmits electronic purchase order 60 to an appropriate location based on an operation that considers business rules associated with the now completed electronic purchase order 60. Continuing with the present example, it will be assumed that electronic purchase order 60 is sent by electronic mail to an approver, D. Little. It is to be noted that, prior to sending the document to D. Little, the method determines that the $100 requested is less than the maximum of $10,000 that D. Little is authorized to approve, as is shown in Table I.

The method shown on Figure 3 is then substantially repeated for the approval stage of the processing of electronic purchase order 60. Continuing with the present example, at step 200, the identity of the authorized user is verified. D. Little inserts her smart card into purchasing intelligent device 44. Similar to step 200 for F. Smith, the user-specific information from the smart card is then transferred to purchasing server 36. Purchasing server 36 then matches the information from the smart card to the user list stored on the persistent storage device of server 36. Again, if the information from the smart card does not match an authorized user from the user list, the respective purchasing intelligent device is not made available by server 36 for use to the user. Continuing with the present example, it is assumed that D. Little's smart card matches an authorized user from the user list in Table I and purchasing intelligent device 44 is made available by server 36 for use by D. Little.

At step 210, the authorized user's privileges are determined. In the present embodiment, server 36 determines that D. Little is given approval privileges as shown in Table I. Further, D. Little is not given request or issuance privilege.

At step 220, D. Little opens her electronic mailbox and finds electronic purchase order 60 in her in-box. D. Little recovers the hash by decrypting F. Smith's affixed digital signature using a public decryption key complementary to the private encryption key of F. Smith. The author and authenticity of electronic purchase order 60 can then be verified by hashing the received electronic purchase order and comparing the result to the decrypted hash. An unverified document can be handled using any desired exception processing technique, such as discarding electronic purchase order 60; returning electronic purchase order 60 to the requester for resubmission with an annotation attached indicating why the document is being returned, or sending electronic purchase order 60 to a security department for investigation.

Referring now to Figure 4, Little can review electronic purchase order 60 and enter or fill-out document data representing either an approval or disapproval (indicated as item 81 on Figure 5) of the electronic purchase order 60 prepared by the requester. In the present example, Little approves electronic purchase order 60.

At step 222, server 36 then compares the data entered at step 221 with the privileges as determined at step 210 and determines whether D. Little was authorized to enter the data that she entered. In the present example, server 36 determines that D. Little has approved electronic purchase order 60 and the method proceeds to step 224.

Note that if D. Little had attempted to enter any data at step 221 that did not accord with her privileges, then the method would loop back to step 221 via step 223 and D. Little would be prompted to enter data that does accord with her privileges.

At step 230, D. Little's digital signature is associated with purchase order 60. Server 36 runs electronic purchase order 60 through a hashing operation which generates a hash. The hash is then converted into a digital signature by encryption of the hash using an encryption key private to D. Little. The digital signature is then affixed to electronic purchase order 60. D. Little can only attach her digital signature to approver signature field 84 according to the privileges as determined at step 210.

At step 240, server 36 transmits electronic purchase order 60 to an appropriate location based on an operation that considers business rules based on electronic purchase order 60. Continuing with the present example, it will be assumed that electronic purchase order 60 is sent by electronic mail to L. Carter.

(Note that if D. Little had approved electronic purchase order 60, server 36 would attach a disapproval notice in field 81 at step 224, and electronic purchase order 60 would be transmitted to the requester, F. Smith at step 240. In the case of a rejection, typically, D. Little would be given an opportunity to attach an email or other type of annotation to the rejected electronic purchase order 60 in order to explain the rejection to the requester, F. Smith.)

The method shown on Figure 3 is substantially repeated for the issue stage of the processing of electronic purchase order 60. Continuing with the present example, returning again to step 200, the identity of the authorized user, in this case the issuer, L. Carter, is verified. L. Carter inserts his smart card into purchasing intelligent device 48. L. Carter's smart card matches an authorized user from the user list and purchasing intelligent device 48 is made available by server 36 for use by L. Carter.

At step 210, the authorized user's privileges are determined. In the present embodiment, server 36 determines that L. Carter is given issuance privileges. Further, L. Carter is not given request or approval privilege.

At step 220, L. Carter opens his electronic mailbox and finds electronic purchase order 60 in his in-box. L. Carter recovers the hash by decrypting D. Little's affixed digital signature using a public decryption key complementary to the private encryption key of D. Little. The author and authenticity of electronic purchase order 60 can then be verified by hashing the

received electronic purchase order 60 and comparing the result to the decrypted hash. As previously discussed, un unverified document can be handled using any desired exception handling technique.

Referring now to Figure 4, L. Carter can review electronic purchase order 60 and fill-out or enter document data representing either an "issued" or "not issued" (shown if Figure 5 as item 82) electronic purchase order 60. In the present example, L. Carter issues electronic purchase order 60.

At step 222, server 36 then compares the data entered at step 221 with the privileges as determined at step 210 and determines whether L. Carter was authorized to enter the data that he entered. In the present example, server 36 determines that L. Carter has issued electronic purchase order 60 and the method proceeds to step 224.

It is to be understood, however that if L. Carter had attempted to change the data in any of data fields 68, 72, 76, the method would move to step 223, the received document data, the method would return to step 221. Similarly, if L. Carter attempted to enter any data that did not accord with his privileges, then the method would proceed to step 223, where the data would be cleared and the method would return to step 221. Continuing with the present example, it is assumed that L. Carter has entered data that he was authorized to enter and therefore the method proceeds from step 222 to step 224 and attaches an "issued" notice in issue field 82 in Figure 5.

Note that if L. Carter did not issue electronic purchase order 60, server 36 would attach a "not issued" notice in issue field 82 and return electronic purchase order to, for example, the requester, F. Smith, or the approver D. Little. Typically, L. Carter would be given an opportunity to attach an annotation explaining why the electronic purchase order 60 was not issued, and/or seeking clarification as to a certain aspect of electronic purchase order 60.

Step 230 is substantially similar to step 230 for the requester and approver stage. L. Carter's digital signature is affixed to purchase order purchase order 60 using an encryption key private to L. Carter. The digital signature is then affixed to electronic purchase order 60. L. Carter can only attach his digital signature to purchaser signature field 92 according to privileges determined at step 210.

At step 240, server 36 transfers the completed electronic purchase order 60 to an appropriate vending server connected by network 32. For the purpose of explaining the present

embodiment, completed electronic purchase order is transferred to vending server 52. A vending user, using vending intelligent device 56 can then open an electronic mailbox and finds the completed electronic purchase order 60. The vending user can process electronic purchase order 60 using known digital signature techniques that are symmetric to the techniques to create electronic purchase order 60. For example, the vending user can recover the hash by decrypting L. Carter's digital signature using a public decryption key complementary to the private encryption key of L. Carter. The authenticity of the document can be verified by recreating the hash and comparing the recreated has with the hash recovered from the digital signature. If the hashes are identical, then the document is considered to be authenticated. When the authenticity of the document is verified by the vending user, the vendor can fill the order.

It will be understood that, in other embodiments of the invention, the verification of the authenticity of electronic purchase order 60 can be substantially automated by computer programs executing on vending server 52. The items in the electronic purchase order 60 can then be automatically placed in a database that schedules those items for shipment from the vendor to the purchaser.

While the embodiments discussed herein are directed to particular implementations of the present invention, it will be apparent that the sub-sets and variations to this embodiment are within the scope of the invention. For example, while there is a single vendor and vending intranet in the above described embodiment, there can be any number of vendors and vending intranets, as will occur to those of skill in the art. Also, there can be any number of purchasers and purchasing intranets. Further, there can be any number of purchasing servers, purchasing intelligent devices, vending servers, and vending intelligent devices. While there are only five authorized users according to Table 1, it will be understood that there can be any number of authorized users. It will also be understood that the other privileges and combinations and permutations of privileges can be assigned to any authorized users. Also, vending intranet and purchasing intranet need not be an "intranet" but can be any type of network, such as a LAN or WAN, etc.

The purchase order shown in Figure 2 is for exemplary purposes only and the information contained in the data fields and the number of data fields can vary. For example the quantity field, item field, and cost field may be columns for the purchase of a number of different items. There may also be a data field to sum the costs listed in the cost column. Date fields may be

assigned when each digital signature is attached to the electronic document and any other field can be added or deleted from the document depending on the business requirements. The number of signatures and the order of processing of the electronic document according to the business rules can vary.

It is contemplated that the privileges shown in Figure 1 are merely exemplary, and that the types and ranges of privileges that are assigned to each authorized user can vary, as desired. Possible types of privileges include, but are not limited to, request privilege, approval privilege, issuance privilege, and maximum cost privilege.

It is contemplated that the present invention can be applied to, for example, the creation, authorizing, approval, review, scheduling, cosigning, counter-signing, editing, transmission, printing of various types electronic documents. Other applications will occur to those of skill in the art.

In certain situations, it can be desired that different types of privileges for the same type of documents are assigned to the same authorized user. For example, where the electronic document is a purchase order, a requester may have higher maximum cost privileges for requests made for capital items and lower maximum costs privileges for requests made for maintenance items. Other examples will occur to those of skill in the art;.

Furthermore, it will now be understood that while the intranets referred to are a purchasing intranet and a vending intranet, the invention described herein can be used for other purposes than just purchasing and vending. Examples of other uses include, electronic invoices, electronic cheques, electronic purchase requests or other business or legal documents, such as contracts, fee estimates, license agreements. For example, the vending company receiving the electronic purchase order can fill the order and complete an electronic invoice and send it to the purchasing company by electronic mail or other suitable electronic data transfer means. Further, an electronic cheque could be completed by the purchasing company to pay for the purchased goods. A new set of privileges and business rules may be associated with these electronic documents.

It is contemplated that the present invention can be applied to other document processing applications where a document may be presented electronically to an individual for approval, where such approval is indicated, represented, or signified by the addition of a digital signature.

Some examples of such an application could include engineering drawings requiring the approval of a professional engineer, or prescription approval by a physician.

It is contemplated that the electronic document can be represented, as it is either stored or transmitted, in a structured tagged-file format, such as the XML format.

It is contemplated that the security or verification protocol for the present invention can include cryptographic cards and/or biometric devices operable to read, for example, thumb-prints or retinas.

The present invention provides a novel method and system for processing electronic business documents. The present invention is believed to be particularly suitable for use in carrying out electronic commerce applications such as purchase orders, company invoices and company cheques. The system and method for processing electronic business documents can require less time to process than some traditional paper systems. The electronic document can be transferred quickly to those individuals in alternate locations and electronic signatures can be acquired very quickly. This includes individuals in other states or countries. Also, individuals who are out of the office can receive the electronic documents, (via, for example, a secure remote connection such as SSL) and associate his or her digital signature with the document and thus allowing for the approval of the document prior to their return to the office or work site. Thus delays to time-critical projects or work can be reduced. Electronic documents can easily be created in multiple languages or translated into a desired language. Copies or records of the electronic document can be saved or sent to each individual or department thus reducing the amount of paper and waste. Further, desired changes to the document can be made electronically and can reduce paper waste. Also, forgery of a document or signature and circumvention of the verification procedure can be more difficult. The present invention can also assist in the reduction of errors in the processing of electronic documents as the automatic routing of documents to appropriate individuals, and the control over the completion of the document in accordance with privileges can assist in avoiding routine errors during the preparation of the document. In addition, the automatic routing of the documents to the appropriate individuals (i.e. authorized users) can ensure a tighter control over the processing of the documents by keeping the document confidential and ensuring that only individuals who need to see the document are actually presented with the document.

We claim:

1. A computer-based method of processing of an electronic document, said method comprising the steps of:

verifying the identity of an authorized user using a predefined verification protocol;

determining a set of privileges associated with said authorized user;

filling-out said electronic document based on inputs provided by said authorized user, said inputs being in accordance with said privileges;

associating a digital signature to said electronic document; and

transmitting said electronic document to an authorized recipient of said electronic documents in accordance with said privileges.

2. The method according to claim 1 wherein said step of associating includes attaching said digital signature to said electronic document.

3. The method according to claim 2 wherein said step of associating includes storing said digital signature and a record of said electronic document in a database

4. The method according to claim 1, additionally comprising the steps of:

requesting one or more additional authorized users to perform additional processing tasks said electronic document; and

attaching additional digital signatures complementary to said one or more additional authorized users upon fulfilment of said tasks of said electronic document;

5. The method according to claims 1 or 4 comprising the additional steps of:

receiving said document; and

authenticating said document using an operation that considers one of said digital signatures and said document.

6. A computer-based method for configuring a set of digital business signing rules for the processing of an electronic document, said document created by at least one user, said method comprising the steps of:

establishing an identity and verification protocol for at least one system administrator;

verifying the identity of one of said at least one administrator using said verification protocol;

establishing an identity and verification protocol for said at least one user based on parameters provided by said verified administrator; and

establishing a set of privileges and authority levels associated with said electronic document for each of said at least one users based on parameters provided by said verified administrator.

7. The method according to claim 6 comprising the additional step of:

establishing at least one task for processing a batch of at least one type of said electronic documents.

8. The method according to claim 7 wherein said electronic document is an electronic financial instrument.

9. The method according to claim 7 wherein the identity and verification protocol for said at least one user includes the use of a smartcard.

10. The method according to claim 1 or claim 6 wherein said privileges include the ability to enter data in at least one electronic data field in said electronic document.

11. The method according to claim 1 or claim 6 wherein said privileges include the ability to edit at least data field in said electronic document.

12. The method according to claim 1 or 6 wherein said privileges include the ability to schedule said document for subsequent processing by an additional user.

13. The method according to claim 1 or 6 wherein said privileges include the ability to approve previously-completed electronic data fields electronic financial instruments, said data fields having been previously completed by an additional user

14. The method according to claim 1 or 6 wherein said privileges include the requirement that a created electronic document be co-signed by one or more additional users.

15. The method according to claim 1 or 6 wherein said privileges include the requirement that a created electronic document be counter-signed by one or more additional users.

16. The method according to claim 1 or 6 wherein said privileges include the ability to endorse a created electronic financial instrument.

17. The method according to claim 1 or 6 wherein said privileges include the ability to transmit a created electronic financial instrument to at least one of a plurality of authorized recipients.

18. A method of modifying a set of digital business signing rules for the processing of electronic documents, said method comprising the steps of:

verifying the identity of at least one authorized administrator using a predefined verification protocol;

determining a set of privileges associated with said verified at least one administrator;

modifying and/or establishing an identity and verification protocol for at least one user based on parameters provided by said verified at least one administrator, and

establishing a set of privileges and authority levels associated with said electronic documents for each of said at least one users based on parameters provided by said verified at least one administrator.

19. The methods claims 1-19 wherein said digital signature is an encrypted hash, said hash being generated based on a hashing operation that considers said electronic document, said encryption being based on a private encryption key private corresponding to said authorized user, said encryption key being complementary to a public decryption key corresponding to said authorized user.

20. A system for processing an electronic document, said system comprising:

a processor operable to verify the identity of an authorized user using a predefined verification protocol;

said processor being further operable to determining a set of privileges stored on a persistent storage device, said privileges being associated with said authorized user;

a user-input device operable to receive data to complete said electronic document, said processor being operable to compare said data with said authorized privileges and reject said data when said data is not in accordance with said privileges;

said user-input device being further operable to receive a request from said user to generate a digital signature corresponding to said user;

said processor being further operable to generate said digital signature;

said processor being further operable to complete said document by associating said signature to said electronic document; and,

said processor being further operable to transmit said completed electronic document for presentation to an authorized recipient.

21. The system according to claim 20 wherein said associating includes attaching said digital signature to said electronic document.

22. The system according to claim 20 wherein said associating includes storing said digital signature and a record of said electronic document in a database

23. The system according to claim 20 wherein said electronic document is an electronic financial instrument.

24. The system according to claim 20 wherein said verification protocol includes the use of a smartcard.

25. The system according to claim 20 wherein said privileges include the ability to enter data in at least one electronic data field in said electronic document.

26. The system according to claim 20 wherein said privileges include the ability to edit at least data field in said electronic document.

27. The system according to claim 20 wherein said privileges include the ability to schedule said document for subsequent processing by an additional user.

28. The system according to claim 20 wherein said privileges include the ability to approve previously-completed electronic data fields electronic financial instruments, said data fields having been previously completed by an additional user

29. The system according to claim 20 wherein said privileges include the requirement that a created electronic document be co-signed by one or more additional users.

30. The system according to claim 20 wherein said privileges include the requirement that a created electronic document be counter-signed by one or more additional users.

31. The system according to claim 20 wherein said privileges include the ability to endorse a created electronic financial instrument.

32. The system according to claim 20 wherein said privileges include the ability to transmit a created electronic financial instrument to at least one of a plurality of authorized recipients.

33. The system according to claim 20 wherein said digital signature is an encrypted hash, said hash being generated based on a hashing operation that considers said electronic document, said encryption being based on a private encryption key private corresponding to said authorized user, said encryption key being complementary to a public decryption key corresponding to said authorized user.

34. The system according to claim 20 wherein said electronic document is one of an invoice, a purchase request, a contract, a fee estimate, a license agreement, an engineering drawing and a prescription.

35. The system according to claim 20 wherein said electronic document is represented in a structured tagged-file format.

36. The system according to claim 35 wherein said electronic document is represented in XML format.

37. The system according to claim 20 wherein said verification protocol includes at least one one of a personal identification number, a cryptographic card and a biometric device.

38. The system according to claim 20 wherein said user-input device is an intelligent device and said processing unit is a server.

39. The system according to claim 38 wherein said intelligent device and said server are part of an intranet.

40. The system according to claim 38 wherein said intelligent device and said server are part of a local area network.

41. The method according to any one of claims 1-19 wherein said electronic document is one of an invoice, a purchase request, a contract, a fee estimate, a license agreement, an engineering drawing and a prescription.

42. The method according to any one of claims 1-19 wherein said electronic document is represented in a structured tagged-file format.

43. The method according to claim 42 wherein said electronic document is represented in XML format.

44. The method according to claim 39 wherein said verification protocol includes at least one one of a personal identification number, a cryptographic card and a biometric device.

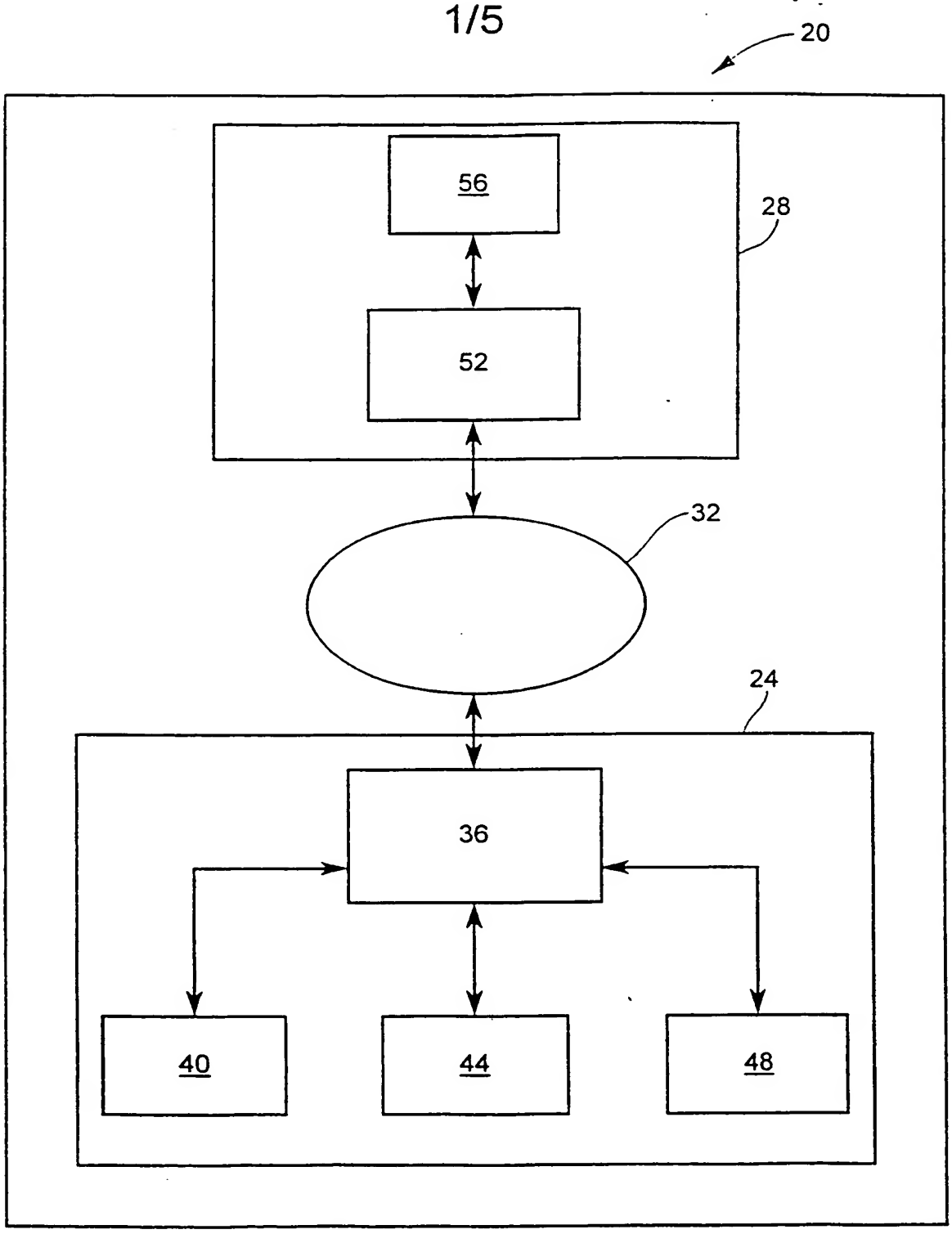



FIG. 1

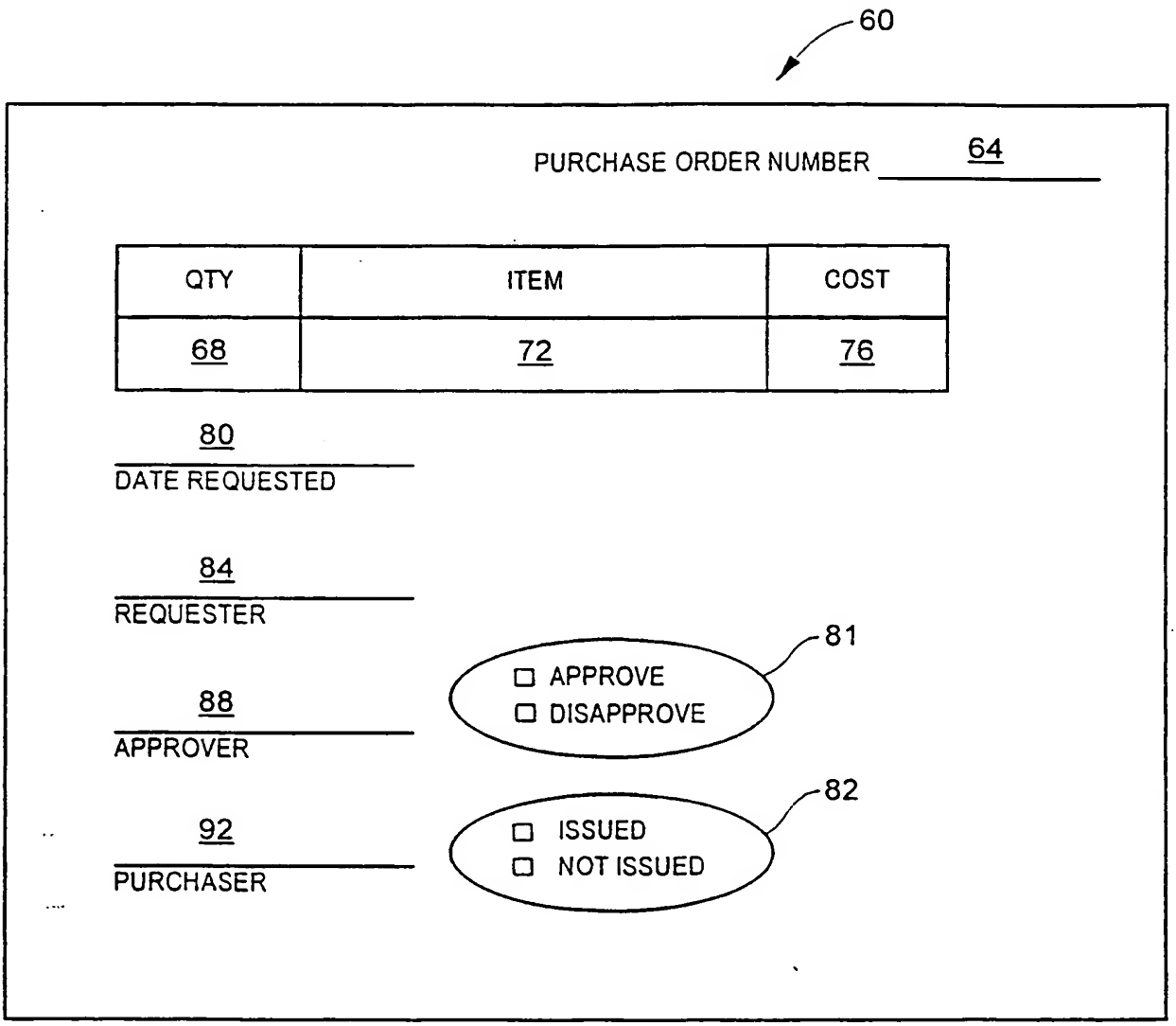

60
PURCHASE ORDER NUMBER 64
QTY
ITEM
COST
68
72
76
80
DATE REQUESTED
84
REQUESTER
81
APPROVE
DISAPPROVE
88
APPROVER
82
ISSUED
NOT ISSUED
92
PURCHASER

FIG. 2

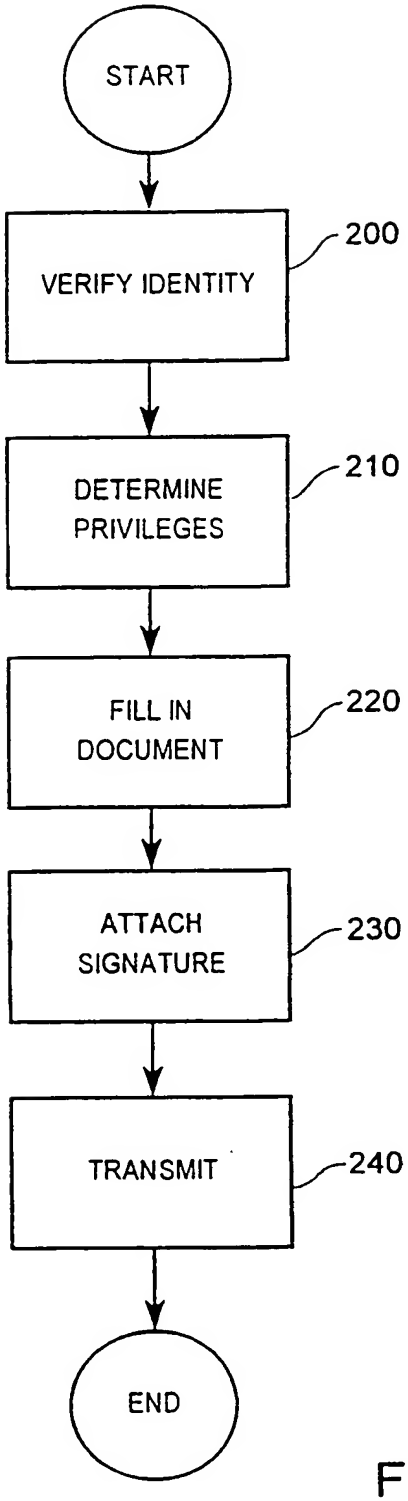

START
VERIFY IDENTITY
200
DETERMINE PRIVILEGES
210
FILL IN DOCUMENT
220
ATTACH SIGNATURE
230
TRANSMIT
240
END

FIG. 3

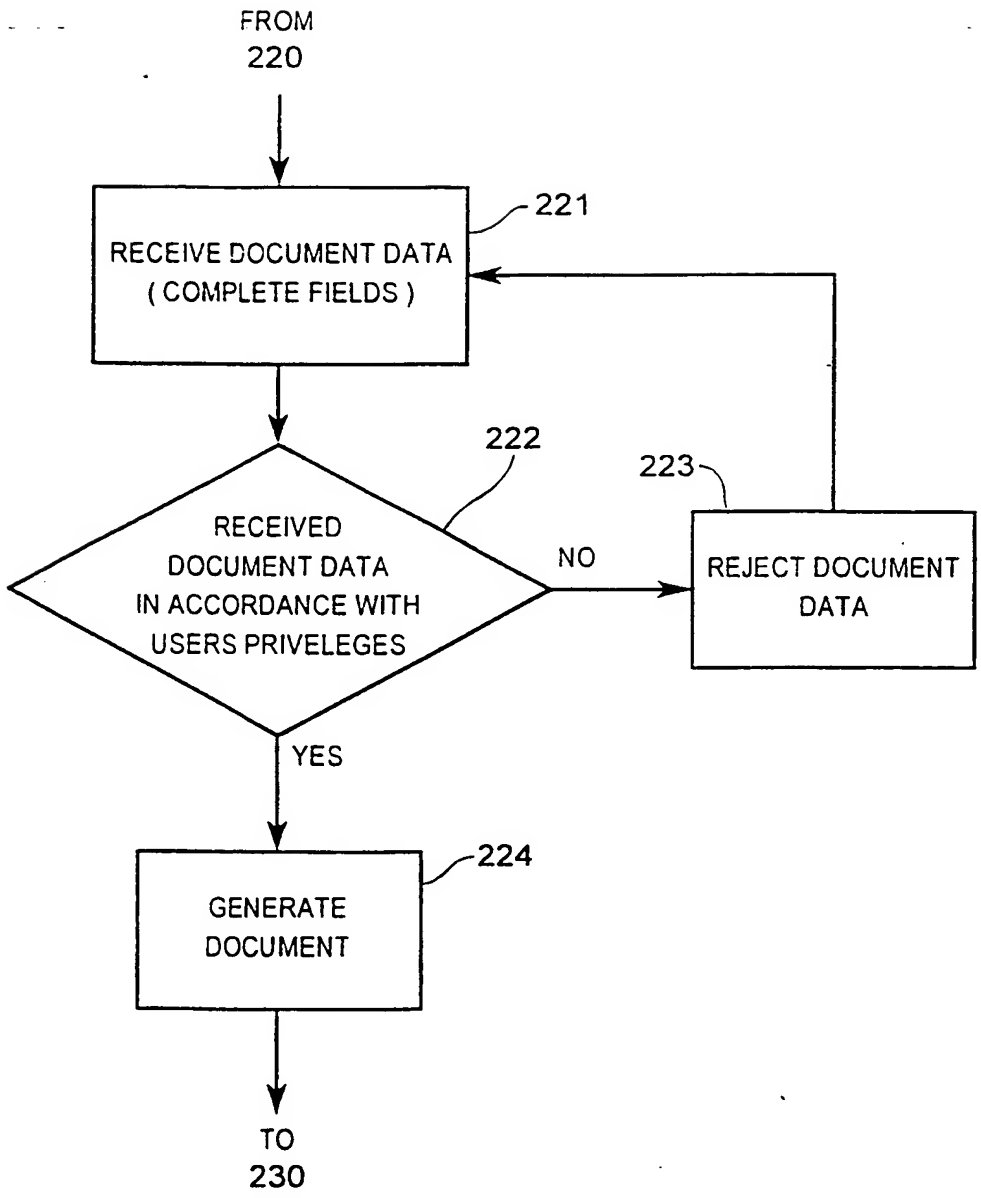

FROM
220
RECEIVE DOCUMENT DATA
( COMPLETE FIELDS )
221
RECEIVED
DOCUMENT DATA
IN ACCORDANCE WITH
USERS PRIVELEGES
222
NO
REJECT DOCUMENT
DATA
223
YES
GENERATE
DOCUMENT
224
TO
230

FIG. 4

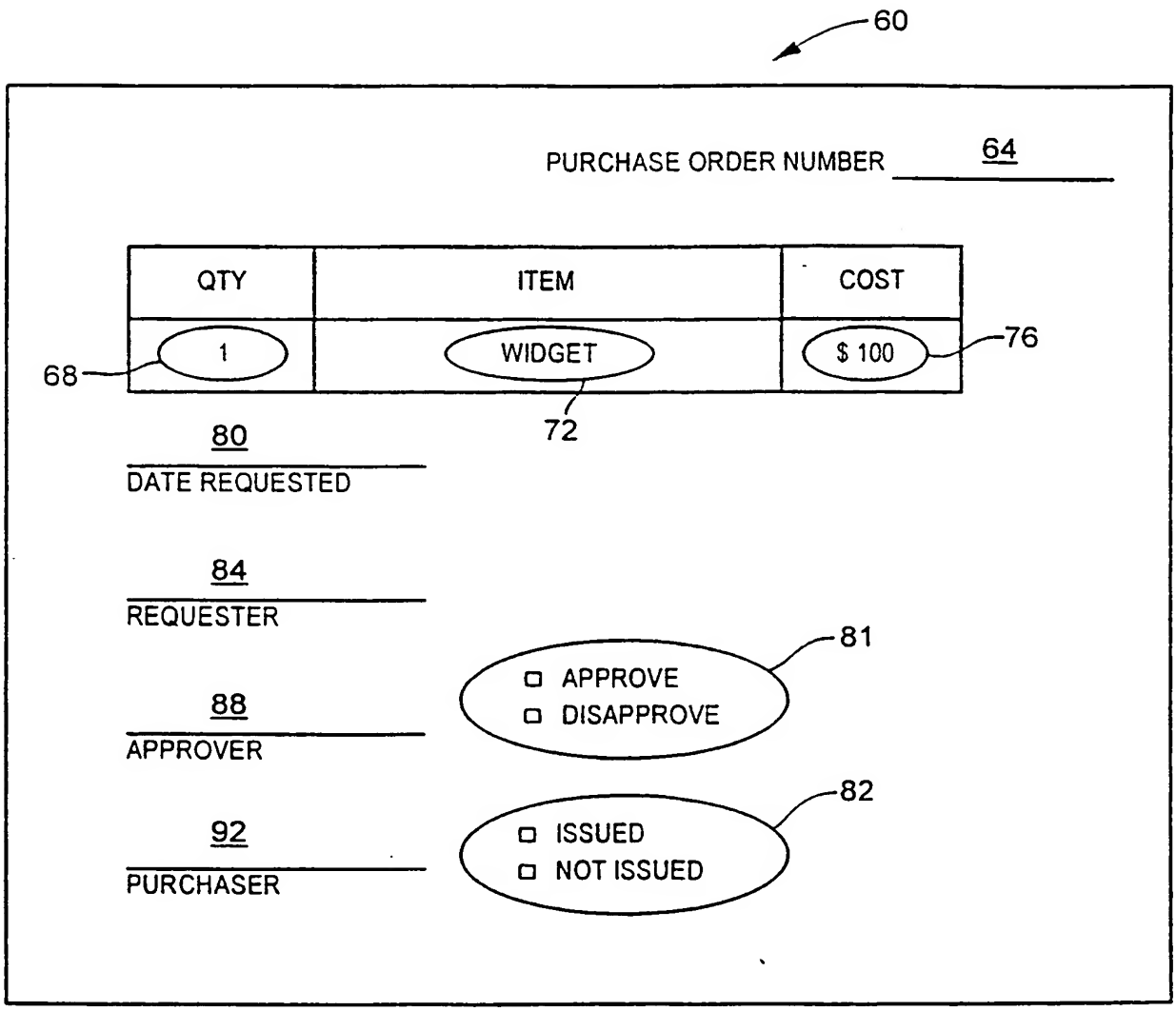

60
PURCHASE ORDER NUMBER 64
QTY
ITEM
COST
1
WIDGET
$ 100
68
72
76
80
DATE REQUESTED
84
REQUESTER
81
APPROVE
DISAPPROVE
88
APPROVER
82
ISSUED
NOT ISSUED
92
PURCHASER

FIG. 5

# INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/CA 00/00291

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/60 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | EP 0 387 462 A (IBM)<br>19 September 1990 (1990-09-19) | 1,2,4,<br>6-8,<br>10-18,<br>20,21,<br>23,<br>25-32,<br>34,35,<br>37-43,45 |
| Y | | 9,19,24,<br>33 |
| A | | 3,5,22,<br>36,44 |
| | abstract<br>page 3 -page 42, line 42<br>figures 1-18 | |
| | -/-- | |

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 20 July 2000 | 26/07/2000 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Jacobs, P |



Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/CA 00/00291

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 5 659 616 A (SUDIA FRANK WELLS)<br>19 August 1997 (1997-08-19) | 1,2,5,<br>10,11,<br>14-17 |
| Y | | 9,19,24,<br>33 |
| A | | 3,4,6-8,<br>12,13,<br>18,<br>20-23,<br>25-32,<br>34-45 |
| | abstract<br>column 9, line 13 -column 18, line 28<br>figures 5-13 | |
| X | EP 0 778 535 A (SUN MICROSYSTEMS INC)<br>11 June 1997 (1997-06-11) | 1-4,6-8,<br>10-18,<br>20-23,<br>25-32,<br>34-45 |
| | abstract<br>column 5, line 20 -column 16, line 9<br>figures 1-7 | |
| A | US 5 465 299 A (MATSUMOTO HIROSHI ET AL)<br>7 November 1995 (1995-11-07) | 1-5,<br>10-17,<br>20-23,<br>25-45 |
| | abstract<br>column 1, line 15 -column 12, line 16 | |
| A | RUSSELL S: "AUDIT-BY-RECEIVER PARADIGMS FOR VERIFICATION OF AUTHORIZATION AT SOURCE OF ELECTRONIC DOCUMENTS"<br>COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM,<br>vol. 13, no. 1,<br>1 February 1994 (1994-02-01), pages 59-67,<br>XP000430128<br>ISSN: 0167-4048 | |

# INTERNATIONAL SEARCH REPORT

information on patent family members

Inte onal Application No
PCT/CA 00/00291

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 0387462 A | 19-09-1990 | DE 68926446 D | 13-06-1996 |
| | | DE 68926446 T | 05-12-1996 |
| | | JP 2278458 A | 14-11-1990 |
| | | US 5315504 A | 24-05-1994 |
| US 5659616 A | 19-08-1997 | AU 698454 B | 29-10-1998 |
| | | AU 3715695 A | 16-02-1996 |
| | | CA 2194475 A | 01-02-1996 |
| | | CZ 9700115 A | 17-09-1997 |
| | | EP 0771499 A | 07-05-1997 |
| | | JP 10504150 T | 14-04-1998 |
| | | NO 970084 A | 10-03-1997 |
| | | TR 970079 A | 21-02-1997 |
| | | WO 9602993 A | 01-02-1996 |
| EP 0778535 A | 11-06-1997 | US 5754857 A | 19-05-1998 |
| | | JP 9265408 A | 07-10-1997 |
| US 5465299 A | 07-11-1995 | JP 6224896 A | 12-08-1994 |